ELITE
COURT REPORTING, LLC

December 11 2023

Rich Walters, Esq.

Shaffer & Shaffer

P.O. Box 3973

Charleston, West Virginia 25339-3973

Re: Jonathan R., et al v. Jim Justice, et al.

Dear Mr. Walters:

Please find enclosed the exhibits to the deposition of Danielle Cox, taken on December 8, 2023. You have requested to not receive a paper version of the transcript. I am providing you with the original exhibits for your records.

If you have any questions regarding this matter, please do not hesitate to call.

Thanks,

Tara Arthur, CCR

Tara Arthur, CCR

Elite Court Reporting, LLC

5010 Dempsey Drive
Cross Lanes, WV 25313
Phone 304.415.1122
martha@elitecourtreporting.net

Service Request : 116774 (Closed)

Employee Network Deprovision

Customer Details:-

Customer: Beth Jarrett
Location:
Email: Beth.Jarrett@wv.gov
Phone: 13045589147

Status: Closed
Urgency:
Team: Enterprise - Account Management
Owner:

Service Request Details:-

Report By:
Charging Account:

Comments: Remove a users current network access when transferring or completely remove access when leaving.

Response Target:
Resolution Target:

Created by: Beth Jarrett on 12/30/2022 1:16:29 PM
Responded by: Internal Services on 1/20/2023 8:00:06 PM

Parameters

Requestor	
Requestor Email (Hidden)	Beth.Jarrett@wv.gov
Request Type	Leaving Employment
Requested For	
Employee ID	E078794
Employee Email	Bill.J.Crouch@wv.gov
Org Level 1	Health and Human Resources
Org Level 2	Health and Human Resources Cabinet Secretary's Office
Org Level 3	Error: Subreport could not be shown.
Effective Date/Time	2022-12-30T18:13:50.0000000Z
Does this person have FACT Access?	
Would you like someone to access this person's email? If so, select the person here	

EXHIBIT 1
WIT: Cox
DATE: 12/8/23
TARA ARTHUR, CCR

	E079974 Beth.Jarrett@wv.gov
If you would like an auto reply on this person's email please type the auto reply here	As of December 30, 2022 I am no longer with the Department of Health and Human Resources. For assistance contact DHHRSecretary@wv.gov.
Email Substitute	Beth.Jarrett@wv.gov
Please enter the name of the person who you would like to access this person's MyDrive files.	
MyDrive SubEmail	E079974 Beth.Jarrett@wv.gov
DAA	Jarrett, Beth

Service Request : 132951 (Closed)

Employee Network Deprovision

Customer Details:-

Customer:	Beth Jarrett	Status:	Closed
Location:		Urgency:	
Email:	Beth.Jarrett@wv.gov	Team:	Enterprise - Account Management
Phone:	13045589147	Owner:	

Service Request Details:-

Report By:		Comments:	Remove a users current network access when transferring or completely remove access when leaving.
Charging Account:			

Response Target:		Created by: Beth Jarrett	on 6/30/2023 10:01:57 AM
Resolution Target:		Responded by: Internal Services	on 7/25/2023 7:00:29 PM

Parameters

Requestor	Jarrett, Beth
Requestor Name (Hidden)	Jarrett, Beth
Requestor Email (Hidden)	Beth.Jarrett@wv.gov
Request Type	Leaving Employment
Requested For	Coben, Jeffrey H
Requested For Name (Hidden)	Coben, Jeffrey H
Employee ID	A026972
Employee Email	jeffrey.h.coben@wv.gov
Org Level 1	Health and Human Resources
Org Level 2	Health and Human Resources Cabinet Secretary's Office
Org Level 3	Error: Subreport could not be shown.
Effective Date/Time	2023-07-05T04:00:00.0000000Z
Requestor Notes	Do Coben has requested his auto reply begin on July 5 as of 12:01am.

Does this person have FACT Access?	⊗
Would you like someone to access this person's email? If so, select the person here	Jarrett, Beth
Substitute Name (hidden)	Jarrett, Beth
	E079974 Beth.Jarrett@wv.gov
If you would like an auto reply on this person's email please type the auto reply here	Effective July 5, 2023, I am no longer serving as Interim Cabinet Secretary for the West Virginia Department of Health and Human Resources. Questions, communication, or other inquiries should be sent to DHHRSecretary@wv.gov.
Email Substitute	Beth.Jarrett@wv.gov
Please enter the name of the person who you would like to access this person's MyDrive files.	Jarrett, Beth
MyDrive Name (hidden)	Jarrett, Beth
MyDrive SubEmail	E079974 Beth.Jarrett@wv.gov
DAA	Jarrett, Beth

Disabled Account Process

Accounts are disabled for various reasons. An account may become disabled only through intervention by the account administrators (this excludes temporary user inflicted suspensions or lockouts.) These disabled accounts may become scheduled for deletion based on the original reason for placing the account into a disabled status.
Reasons for an account becoming disabled (excluding dormant accounts):

- Employement separation, terminations, leave of absence, or disciplinary action
- Security requests for terminations, leave of absence or disciplinary action
- Critical time sensitive actions directed from HR, Security or managers for employee/contractor terminations or disciplinary actions (must be followed up by a security request form)

Disabled Accounts will be purged after being disabled 30 calendar days. This includes home directories, data sets, emails files and accounts. No extensions will be accepted *after* 30 days and accounts will be purged accordingly.

Disabled accounts due to leave of absence will be reinstated as directed by HR or supervisors via a security request form. Accounts disabled due to leave of absence will not be deleted unless notification is received from HR or supervisors via a security request form that the employee has been terminated.

Disabled accounts due to disciplinary action will be reinstated as directed by HR or supervisors via a security request form. Accounts disabled due to disciplinary action will not be deleted unless notification is received from HR or supervisors via a security request form that the employee has been terminated.

WEST VIRGINIA office of technology

ESS Policies, Standards, Procedures and Guidelines: Enterprise Productivity Suite / Enterprise Lifecycle Management Procedure

Effective Data: 2/23/2022

Introduction

Lean methods teach us that a key to reducing waste is to adopt standard work processes. If data or business processes are similar across state government agencies, it is important to consider whether standardization could provide efficiencies or enable new capabilities for the enterprise. In West Virginia, data, business processes and technologies are required to be standardized across the enterprise.

Purpose

Defines a process and lays the foundation for governance, decision making and agency involvement in services or systems.

Establishing a process enables the service to reasonably assume a large customer base and a more predictable adoption rate from the beginning. This enables:

- The process to derive economies of scale and/or efficiencies from subsequent planning, analysis, and decision making.
- Customer agencies provide input to the process and participate in decisions encouraging a customer-obsessed culture within the West Virginia Office of Technology.

Procedure

Onboarding/Provisioning

- Agency submits employee details to the service desk via a Service **Request.(Employee Network Account Request)**
- User created in Active Directory, assigned group permissions, account is created
    - Accounts Management must populate the email attribute in ARS for the user to get synced to Google and to get a mailbox.
- [redacted]

EXHIBIT 4
WIT: Cox
DATE: 12/8/23
TARA ARTHUR, CCR

Watchpoint

- [redacted]
- GCDS will not create a new user account if there is not an available Google Workspace license.

- [redacted]

Extended Leave

- To suspend - Agency submits employee details to the service desk via an Ivanti Form.(Employee Temporary Disable or Enable)
  - [redacted]
- To reactivate - Agency submits employee details to the service desk via an Ivanti Form.(Employee Temporary Disable or Enable)
  - [redacted]

Offboarding/Termination at Agency Level

- Agency submits employee details to the service desk via an Ivanti Form.(Network Deprovision Request)
- Disable account in AD
  - [redacted]
- If Delegating access to an Executor,
  - Delegate Access to the Departing User's Email (Default is 30 days)
    - The account Executor will need access to any pending correspondence in the departing user's mailbox, especially if the departure was sudden or occurred on less than friendly terms. Fortunately, you can designate access to a Gmail

account to anyone else on your domain. The delegate - who, again, will likely be the Executor -- won't be able to change account permissions, passwords, or chat on the original user's behalf, but the delegate can send and receive mail from the account until it is suspended or deleted upon agency request.

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- [redacted]
- [redacted]
  - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
  - [redacted]

- Wipe the Mobile Device(s)
  - Wipe is by special request only via call/email to the service desk. Once, incident is entered the identified device is wiped via Google admin center.

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

- Transfer Drive Ownership of the Departing User's Google Docs

  NOTE: *When the account that owns a Google Doc is deleted, that document is deleted as well--even if it was shared with other domain users. Put more simply, deleting a user deletes every critical document that user ever created. Fortunately, the Admin Panel offers a method to bulk-transfer ownership of all the user's Google My Drive documents to another domain user's account. In other words, you can make the Executor the owner of all a departing user's Docs in a matter of seconds, ensuring that this data stays online and accessible even after the original owner is de-provisioned. The Executor can then transfer individual ownership on a case-by-case basis.*

WEST VIRGINIA office of technology

ESS Policies, Standards, Procedures and Guidelines: Enterprise Productivity Suite / Enterprise Lifecycle Management Procedure

Effective Data: 2/23/2022

Only files owned by a user can be transferred to another user, who becomes the new owner.

The hierarchy structure of the previous owner is the same in the new owner's Drive.

Existing shared documents are not affected by the transfer.

Some files are not moved:

Google Photos and Maps are not transferred.

Files and folders in the user's Trash are not transferred, so move files out of the Trash, if they should be retained. Otherwise, files in the Trash are deleted when a user is deleted.

Orphan files (Google Photos and Maps) are not moved, so move them to the user's My Drive, if they should be transferred:

In the Drive search field, type: is:unorganized owner:<username>

Move any orphaned files found to the user's My Drive.

- Delegate Access to the Departing User's Calendars
  - If the departing user managed a shared calendar, or simply had a series of company appointments that the Executor must now manage, it is important to transfer control of those calendars. Simply log in as the departing user, and then follow the Share With Specific Users instructions to give the Executor the Edit Events and Manage Sharing access level for the appropriate calendars. The Executor can then assign calendar permissions as needed. More information.

- If User returns to work in a different Department, or a different Agency based on policy
  - Best practice is to start these returned users with a brand new account.
    - [redacted]

[redacted]

- If a user returns before 25 days after account deletion in Google, the account can be restored from Google Admin.
    - Any data that was remaining in that account will be restored. (Drive, Calendar, Gmail, Tasks)
- If Drive data was transferred to a new owner (Executor), that data **cannot** automatically be transferred back to the original owner. The suspended user (after activation) will retain edit access to previously owned documents if the new owner has not changed these sharing settings.
- The new owner of the files would need to change the ownership on a document-by-document basis in order to transfer files back to the original owner.
    - [redacted]

[redacted] Users will remain in a suspended state until 30 days have passed. After 30 days, admins can delete the account in the admin panel or in bulk using GAM.

- Only Drive, Calendar and Data Studio assets can be transferred to a new owner at deletion.
    - If other service data is needed to be transferred, a manual export must be used with one of the following options, Google Takeout or via Vault Export.

WEST VIRGINIA office of technology

ESS Policies, Standards, Procedures and Guidelines: Enterprise Productivity Suite / Enterprise Lifecycle Management Procedure

Effective Data: 2/23/2022

Litigation Hold

- Create Matters in Google Vault
- Setup Litigation Hold in Google Vault
- Manage custom retention rules in Google Vault
- Disable account in AD
  - [redacted]
- Move disabled account on litigation hold into an OU [redacted] This is for ease of administration and eventual deletion (freeing up a license).
- Account will remain in [redacted] OU until the time that this data is not needed to be retained in Vault.
- Once an account is not needed data can be transferred to a different account or the account can be deleted, freeing up a license.

MDM Request

[redacted]

WEST VIRGINIA office of technology

ESS Policies, Standards, Procedures and Guidelines: Enterprise Productivity Suite / Enterprise Lifecycle Management Procedure

Effective Data: 2/23/2022

[redacted]

Google Groups

- No change in current process (Calendars, DLs, Security Groups)
- Google Group SOP

Google Shared Drive Creation

- If managed by WVOT,
  - Agency submits employee details to the service desk via an NAF Google Drive Request Form.
- If management is requested by the Agency,
  - Agency submits employee details to the service desk via an NAF Elevated Rights Request Form.
  - User assigned to Google **Shared Drive Creators** group.
- Google Shared Drive SOP

WEST VIRGINIA office of technology

ESS Policies, Standards, Procedures and Guidelines: Enterprise Productivity Suite / Enterprise Lifecycle Management Procedure

Effective Data: 2/23/2022

Change Recommendations

Change recommendations are encouraged to foster a continuously improving and efficient process. If you are aware of any changes or improvements that should be made in response to a business change or opportunity to automate, please bring these recommendations to your immediate supervisor.

Supervisors will present any recommendations to senior management for consideration, approval and implementation.

State of West Virginia Office of Technology Procedure:

Technical Investigation Request

Issued by the CTO

1.0 PURPOSE

The purpose of this Procedure is to specify the process for State agencies when requesting an investigation into any State employee's technology-based activity. **This procedure should not be construed to convey any expectation of privacy.**

2.0 SCOPE

This procedure applies to all Departments (including agencies, boards, and commissions) within the Executive Branch of West Virginia State Government, excluding constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, and the county boards of education. However, the West Virginia Office of Technology (WVOT) recommends that all Agencies, including those excluded above, follow this procedure.

Supervisors and managers must follow this procedure to initiate investigations of persons using State equipment and systems.

3.0 REQUIREMENTS

3.1 To gain access to information about employees' technology-based activities, a suspected violation of law or policy should be identified to initiate the required technical investigations.

3.2 Any supervisor or manager may initiate a **request** for access. However, only Office Directors, Commissioners, Cabinet Secretaries, or the *Legislature's Commission on Special Investigations have the authority to **approve and submit** requests for investigations of staff in their **own** office, agency, or department. (**may request from any office*)

3.3 Agencies should exercise discretion when requesting reports of user activities, and should involve both Agency Legal and Personnel services in the decision to submit such requests.

3.4 The Service Desk, or any WVOT employee, must immediately transfer all investigation requests to the Cyber Security Office (CSO).

3.5 All employees involved in technical investigations are required to keep all information discovered in the process confidential.

4.0 PROCEDURE

4.1 ALL investigation requests must be submitted to WVOT through electronic email with the form in Attachment A to James.D.Kirk@wv.gov and James.L.Amos@wv.gov.

4.2 When requesting a technology-related investigation for any State employe

e

the following information must be submitted to James.D.Kirk@wv.gov and James.L.Amos@wv.gov:

4.2.1 Name, title, agency name, and phone number of the supervisor or manager requesting the investigation;

4.2.2 Name, e-mail address, and userid of the individual whose activity will be investigated;

4.2.3 Purpose of Investigation or Suspected Violation (ex: to confirm suspicion of abuse or misuse; to remove cloud of suspicion, to validate user presence, etc.) As a guide to the kinds of violations that merit investigation, examples include, but are not limited to the following:

4.2.3.1 Suspected violations of the law. Examples include, but may not be limited to the following:

- Criminal enterprise;
- Sexual harassment; and
- Willful misuse of legally protected information, etc.

4.2.3.2 Suspected violations of State policy. Examples include, but may not be limited to the following (For more information, see "Appendix A" of WVOT-PO1001 - *West Virginia State Information Security Policy*:

- Determination of excessive personal use;
- Commercial enterprise purposes or for-profit activities;
- Sexually explicit use;
- Chain letters;
- Behaviors that introduce viruses or other malware;
- Disabling security systems or controls; and
- Breach of confidentiality, unethical conduct.

4.2.4 Interval of Investigation (ex: 03/01/06 to 08/15/06); and

4.2.5 Report Due Date (based upon urgency).

4.3 If it becomes necessary to expedite the delivery of a request, the Chief Information Security Officer (CISO) or, if the CISO is unavailable, the Chief Information Officer (CIO) should be contacted for immediate assistance. 4.

4 The CISO will work with other Directors as needed to assign investigative tasks to the appropriate technicians.

4.5 The WVOT will perform a best-effort investigation over the specified interval to determine the existence of findings that could indicate a violation. The authorized requestor agrees to the following:

4.5.1 The WVOT may utilize any sources, tools, or technologies needed to provide the most accurate, detailed, and relevant information possible;

4.5.2 The individual under investigation will remain separated from the investigator at all times; and

4.5.3 All acquired materials and data gathered will remain in the custody of the investigator. Materials may be acquired in two ways:

- Remotely (requires chain of custody form)
- On-Site

4.6 The CISO will send the authorized requestor a detailed report of the findings resulting from the investigation. This will follow the same path as the request (technician –CISO– requestor). A copy of the report may (when warranted) also be forwarded to the Agency Personnel Office and the West Virginia Division of Personnel. Criminal activity findings may be reported directly to law enforcement.

4.7 Agencies using investigative services provided by the WVOT may be billed according to a standard rate structure.

5.0 ENFORCEMENT

Not applicable to this document

6.0 DEFINITIONS

6.1 Cabinet Secretary – The leader of a Department appointed by the Governor.

6.2 Chief Information Security Officer (CISO) - Person designated by the CTO to oversee Information Security practices and initiatives for the Executive Branch of WV State government, excluding the constitutional officers.

6.3 Chief Information Officer (CIO) – The person responsible for the State's information resources.

6.4 Commissioner - The leader of a State organizational entity (Bureau, Commission, etc.)

6.5 Contractor – Anyone who has a contract with the State or one of its entities.

6.6 E-mail – Any message sent electronically through one or more computers and/or communications networks, and in most cases has a human originator and receiver.

6.7 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.

6.8 Legislature's Commission on Special Investigations – The group charged with performing a range of investigative tasks, including suspected purchasing violations, illegal conduct by State employees, conflicts of interest, bribery of State officials, and malfeasance. This body may also recommend action to the Attorney General, prosecuting attorney, or other authority empowered to act upon such recommendation. (See http://www.legis.state.wv.us/Joint/Special_Investigations/csi_mission.cfm)

6.9 Malware - Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a blend of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

6.10 Office Director – The designated or appointed leader of a state organizational entity who generally reports directly to the head of the agency, such as a Commissioner.

6.11 Cyber Security Office (CSO) - The functional unit charged with the responsibility to undertake and sustain initiatives to promote, enhance, monitor, and govern actions, standards, and activities necessary to safeguard data and information systems within the Executive Branch of WV, as provided in West Virginia Code §5A-6-4a and the Governor's Executive Order No. 6-06.

6.12 Procedure – A series of steps followed in a definite regular order ensuring the consistent and repetitive approach to actions.

6.13 Userid – A unique "name" by which each user is identified to a computer system.

6.14 West Virginia Division of Personnel – The Division of the Department of Administration established by WV CODE § 29-6-1 *et seq.*, which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.

6.15 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, et. seq., which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

7.0 Change Log History

- January 30, 2015 – Added Change Log History
- 9/1/2016 – Policy Reviewed. No edits made.
- 10/20/2017 – Policy Reviewed. Minor text edits made.
- 04/24/2022- Updated contact information and Appendix

State of West Virginia Office of Technology Procedure:

Appendix A:
Technical Investigation Request Form

Issued by the CIO

Requesting Technical Investigation/Information

****Sections 1 through 3 must be filled out by Supervisors or Managers Only****

Section 1

1. Supervisor or Manager Requesting Investigation:
2. Title: 3. Agency:
4. Phone # 5. Email:
6. Billable PAS #

Section 2 (If a person is being investigated)

1. Name of Individual to be Investigated:
2. Email: **3. UserID:**

Section 3

1. Purpose of Investigation or Suspected Violation:
(see 4.1.3 of WVOT-PR1001, attach additional pages if necessary to explain)
2. Interval of Investigation From: To:

Section 4

This section must ONLY be filled out by a Cabinet Secretary, a Commissioner, an Office Director, the Office of Special Investigations, or an Equivalent Authority (e.g. GEIST Member):

1. Has the Technical Investigations procedure been read and understood? Yes No
2. Has the requestor provided sufficient information to initiate this investigation? Yes No
3. Does your Agency require Legal and/or Personnel approval for investigation actions? Yes No

7. Agency:
8. Email: 9. Phone:
10. Signature: 11. Date:

This form must be forwarded to the Chief Information Security Officer (CISO) along with ALL supporting documentation. Send by Fax: 304-957-0137 OR Mail: West Virginia Office of Technology, Building 5, 10th Floor, 1900 Kanawha Blvd., Charleston, WV 25305, Attn: CISO

STATE OF WEST VIRGINIA
DEPARTMENT OF HEALTH AND HUMAN RESOURCES
Office of the General Counsel

Bill J. Crouch
Cabinet Secretary

April L. Robertson
General Counsel

LITIGATION HOLD

ATTORNEY-CLIENT PRIVILEGED

TO: Bill J. Crouch, Cabinet Secretary
Jeremiah Samples, Deputy Secretary
Linda Watts, Commissioner, BCF
Cammie Chapman, Associate General Counsel, BCF
Tanny O'Connell, Deputy Commissioner, BCF
Tina Mitchell, Deputy Commissioner, BCF
Janie Cole, Interim Deputy Commissioner, BCF
James Weekley, Administrative Services Manager, BCF
Shaun L. Charles, Chief Information Officer, Management Information Services
Chris L. Avis, Cyber Security Operations Analyst, WV Office of Technology

EXHIBIT 6
WIT: Cox
DATE: 12/8/23
TARA ARTHUR, CCR

FROM: April Robertson, General Counsel AR

DATE: December 4, 2019

RE: ***Jonathan R. v. Justice, et al.*: DHHR Management of West Virginia's Foster Care Program**

DHHR faces a broad legal challenge to how it manages West Virginia's foster care program, in a case before the U.S. District Court for the Southern District of West Virginia called *Jonathan R. v. Justice, et al.* Plaintiffs currently represent the interests of 12 foster children, and counsel seeks to certify a class of all current and future children in DHHR custody.

As a result of this litigation, DHHR has a legal duty to preserve, and you and the DHHR employees and contractors under your supervision should preserve and maintain, all documents regarding DHHR's management of the foster care program, including documents related to: the kinship program; residential placements; transition planning for individuals aging out of foster care; services for children with serious mental or behavioral disorders; foster home recruitment and certification; the development of case plans and permanency plans; the appointment of counsel and other representatives; case worker training and case load levels; and case files of, and any other information relating to, individual children in DHHR custody.

This duty to preserve includes all paper information, electronically stored information, audio recordings, video recordings, tangible items (written, audio, video, photographs, or other), and other potential information that is or may be relevant to the lawsuit. This includes preservation of items, including, but not limited to the following: (1) e-mail and attachments; (2) text messages and attachments; (3) social media postings; (4) any items maintained on a computer hard drive; (5) any tangible items maintained

using any resources provided by DHHR; (6) any tangible items maintained on your personal computer, personal cellular phone, personal e-mail, personal notes, or otherwise stored on non-business sources that may be relevant to this lawsuit; (7) word processing documents; (8) notes; (9) electronic and non-electronic calendars, diaries, or tasks; (10) databases; (11) time cards and payroll items; (12) voicemail messages; (13) personnel folders, leave information, benefits information, and other employment-related information; (14) policies and procedures; and (15) any computer equipment used by any current or former employee that is in your possession, which may contain information that may be relevant to the lawsuit.

Please note that the above-noted lists **ARE NOT ALL-INCLUSIVE** and err on the side of preservation regarding ANY information that may be relevant to the present lawsuit.

You are to **IMMEDIATELY** preserve and retain all potentially relevant evidence. You are further directed to ensure that any and all persons who you believe may have information regarding this matter maintain that information in its current form to preserve and retain all potentially relevant evidence.

Any person subject to this litigation hold **MUST NOT** alter, delete, destroy, or otherwise modify any tangible items (written, audio, video, computer information, photographs, or otherwise) that may be relevant to the lawsuit until this litigation has concluded. Your obligation to preserve extends to all potentially relevant items in your personal possession, control, or custody, ***including items in possession or custody of employees who report to you or those in the custody of third parties.***

Please also ensure that should items be maintained on your computer desktop, cellular phone, or other medium wherein there is a potential that the medium containing these items could be damaged, which could potentially result in the destruction of relevant evidence, that you are directed to ensure that an exact copy of the information is maintained and preserved by a separate source.

The Department takes this preservation directive very seriously. The litigation hold overrides any routine retention or destruction policies that you currently follow.

This litigation hold SUPERSEDES any and all other formal or informal record retention policies, destruction policies, and business practices regarding destruction of information until this litigation has concluded. If there is a formal or informal document retention policy, destruction policy, or other business practice regarding the destruction of information, you are directed to SUSPEND any and all policies until the litigation has concluded.

Upon receipt and review of the attached letter, please sign the attached Acknowledgment and return to me promptly via e-mail. **If you know of employees who have information and they are not specifically named in this memorandum, please discuss this litigation hold with them and have them execute the attached acknowledgement.**

If you have any questions regarding this litigation hold, you may call me at 304.558.9149.

ACKNOWLEDGMENT

I have reviewed and understand the Litigation Hold dated December 4, 2019, regarding *Jonathan R. v. Justice, et al.*, and agree to abide by and follow the directives contained in the Litigation Hold.

NAME PRINTED: _____

POSITION: _____

SIGNATURE: _____

DATE: _____

State of West Virginia Office of Technology
Procedure: Account Management
Issued by the CTO

Procedure No: WVOT-PR1010 **Issue Date: 03.28.07** **Revised: 08.12.09** **Page 1 of 8**

1.0 PURPOSE

This procedure addresses the responsibilities of the West Virginia Office of Technology (WVOT) with regard to the creation, the authorization, and the modification of network user accounts.

2.0 SCOPE

This procedure applies to all WVOT employees and customer agencies.

3.0 REQUIREMENTS

3.1 WVOT Responsibilities

3.1.1 The WVOT is responsible for provisioning network user accounts by adding, modifying, and deleting user access for customer agencies.

3.1.2 Account request forms will be processed within two working days of receipt.

3.1.3 All designated agency contacts will receive training from the WVOT regarding this procedure.

3.2 Designated Approval Authority

3.2.1 Each agency will appoint one (or more) employees to serve as designated approval authority. This employee(s) will authorize all access modifications for that agency.

3.2.2 According to the needed modification, the designated approval authority will complete a Network Logon Request form(s). (For

more information, see attachment A, the "Network Logon Request Form", and attachment B, the "Network Logon Request Form Instructions".)

3.2.2.1 Paper forms are available by either contacting the WVOT Service Desk at 304-558-9966 or by email at: servicedesk@wv.gov.

4.0 PROCEDURE

4.1 Adding a User ID

4.1.1 When adding a user id, the designated approval authority will complete the following steps:

4.1.1.1 Choose the option *Add Employee.*

4.1.1.2 Specify the type of add(s) (Network, E-mail, etc.).

4.1.1.3 Complete all relevant fields.

4.1.1.4 After the form has been completed, the designated approval authority will submit the form(s) to the WVOT, adhering to the instructions included with the network logon request form.

4.1.1.5 The WVOT will process the request, and will create the requested accounts and access rights.

4.1.1.6 The WVOT will notify the designated approval authority with a verification e-mail when the action has been completed.

4.2 Modifying a User ID

4.2.1 When modifying a user id, the designated approval authority will complete the following steps:

4.2.1.1 Choose the option *Modify Employee*.

4.2.1.2 Specify the type of modify(s) (Network, E-mail, etc).

4.2.1.3 Complete all steps as shown in 4.1.1.3 through 4.1.1.6 of this procedure.

4.3 Deprovisioning a User ID (See 4.3.2)

4.3.1 When deleting a user id, the designated approval authority will complete the following steps:

4.3.1.1 Choose the option *Delete Employee*.

4.3.1.2 Detail the type of delete(s) (Network, E-mail, etc).

4.3.1.3 Complete all steps as shown in 4.1.1.3 through 4.1.1.6 of this procedure.

4.3.2 When an employee leaves the agency under any circumstance, unless an authorized arrangement is made between the agency and the WVOT to preserve access for the employee, the following steps must be taken:

4.3.2.1 The agency authority must contact the WVOT Service Desk, and request all associated accounts be disabled immediately.

4.3.2.2 The designated approval authority will then complete and submit the Network Logon Request form following the "deleting a user id" procedure as listed in 4.3.1.

access the data by contacting the WVOT Service Desk.

4.5.1.1.1 The Account Management Team will contact the requestor to gain specifics of the requested information, and obtain the approval of the appropriate designated approval authority.

4.5.1.1.2 The Account Management Team will make a copy of the file(s) and provide that information to the requestor.

4.5.1.1.3 Requests for access to data of transferring employees must be made within 10 business days.

4.5.1.2 **Other routine business Use:** If a user has left employment, or transferred to an agency outside the WVOT customer base (Executive Domain), the Account Management Team will grant access to the user's specific data during the de-provisioning process after approval has been obtained by the appropriate designated approval authority.

4.5.1.3 Investigative Requests

4.5.1.3.1 To gain access to information about employees' technology-based activities, a suspected violation of law or policy should be identified to initiate the required technical investigations.

4.5.1.3.2 For more information, see WVOT-PR1001 – *Requesting Technical Investigations*

4.6 Deleting Inactive Accounts

4.6.1 In order to mitigate security risks, user accounts will be deleted after 60 days of inactivity and marked as "deleted due to inactivity."

4.6.2 To re-activate the account, the agency Designated Approval Authority must contact the WVOT Service Desk.

5.0 ENFORCEMENT

Any employee found to have violated this procedure may be subject to disciplinary action up to and including dismissal. Disciplinary action, if determined to be necessary, will be administered by the employing agency and may be based on recommendations of the WVOT and the West Virginia Division of Personnel intended to address severity of the violation and the consistency of sanctions.

6.0 DEFINITIONS

5.1 Access – The ability to read, write, modify, or communicate data/information or otherwise use any system resource.

5.2 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

5.3 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.

5.4 Procedure – A defined series or sequence of steps followed in a definite regular order ensuring the consistent and repetitive approach to actions.

4.3.3 All deleted accounts will follow this protocol:

4.3.3.3 The account(s) will be disabled but left intact for 30 days in case access or re-authorization is needed.

4.3.3.4 After 30 days the disabled account(s) will be deleted.

4.4 Access Revocation

4.4.1 Access must be suspended when an employee is on an extended leave of absence and will not be accessing the network. The following steps will be taken:

4.4.1.1 The designated approval authority will complete a modification request, which indicates the type of action (Temporary Disable / Enable Employee) to be completed.

4.4.1.2 The form(s) will be submitted to the WVOT.

4.4.1.3 The WVOT will process the form(s) and notify the designated approval authority by email when the action has been completed.

4.4.1.4 The employee's access to all systems, except e-mail, will be disabled for the appropriate time period.

4.5 Access to a User's Specific and/or Personal Data

4.5.1 Access to a user's home directory or any other specific data may be requested under the following circumstances:

4.5.1.1 **Routine business Use within the Executive Domain:** In the event a user is out of the office, or is transferred to another agency within the Executive Domain and the data is needed to continue routine business operations, a request may be made to

5.5 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, *et. seq.*, which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

6.0 INDEX

Procedure: Account Management
State of West Virginia Office of Technology

State of West Virginia Office of Technology Policy: Account Management

Issued by the CTO

1.0 PURPOSE

This policy will establish a standard for the administration of computing accounts that facilitate access or changes to State of West Virginia (State) Executive Branch data. This policy will also establish standards for creating, issuing, removing, monitoring, and managing employee accounts.

2.0 SCOPE

This policy applies to all departments (including agencies, boards, authorities, and commissions) within the Executive Branch of West Virginia State Government, excluding constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, and the county boards of education using contractor services. However, the West Virginia Office of Technology (WVOT) recommends that all agencies - including those excluded above - follow this procedure.

3.0 POLICY

3.1 The WVOT is responsible for adding, modifying, and deleting network users' account access for Executive Branch agencies. Name changes, accounting changes, and permission changes are all documented.

3.2 All accounts must include a written and authorized Network Logon Request Form, with proper approval documented. User accounts will not be activated until the authorization process and required documentation is completed.

3.3 The WVOT will issue a unique account to each individual authorized to access a particular networked computing and information resource and will promptly deactivate accounts when necessary. (See WVOT-PR1010 – "Account Management" for more information.)

3.4 When establishing accounts, standard security principles of "least privilege access" to perform a function must always be used, where administratively feasible.

3.5 Each agency must have a documented process for periodically reviewing existing accounts to ensure that access and account privileges are proportionate with job function, need-to-know, and employment status. WVOT reserves the right to perform audits on an ad hoc basis. (See WVOT-PO1008 – "Information Security Auditing Program" for more information.)

3.6 Each Executive Branch agency will appoint one (or more) employee(s) to serve as a designated approval authority. This individual(s) will authorize all access modifications for that agency and must complete a Network Logon Request Form, which can be obtained by either contacting the WVOT Service Desk at 304-558-9966 or by email at: servicedesk@wv.gov.

3.7 Agencies must monitor and regularly update approval authorities.

3.8 Those responsible for access to systems/applications/servers, etc. protected by high-level super-passwords (or the equivalent) must have proper auditable procedures in place to maintain custody of those "shared secrets" in the event of an emergency and/or should the super-password holder become unavailable. These documented procedures, which must be appropriately secured, should delineate how these passwords are logically or physically accessed as well as who in the chain-of-command will become responsible for access to and/or reset of the password.

3.8.1 When the employee status of personnel who have access to super-passwords changes, the passwords **must** be changed. Changes in employee status include, but are not limited to: termination, resignation, retirement, and change of departments or agencies.

3.9 Temporary accounts (those used by contractors, vendors, interns, etc.) will be granted on a need-to-use basis following the principle of least privilege.

3.10 Temporary accounts will contain an expiration date of one year or the work completion date, whichever occurs first.

3.11 All temporary accounts must be sponsored by the appropriately authorized member of the administrative entity managing the resource.

3.12 All temporary accounts must be designated as such, so users of those accounts cannot be mistaken for full-time state employees.

3.13 Use of shared accounts is not allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g., management of file shares).

3.13.1 Exceptions will require documentation to justify the need for a shared account. It should include a list of individuals who have access to the shared account. The list will be reviewed at appropriate and documents intervals.

3.13.2 The system owner is responsible for the documentation, and a copy will be shared with WVOT.

3.13.3 The documentation must be available upon request for an audit or a security assessment.

3.14 Application and System Standards

3.14.1 Where technically or administratively feasible, shared ID authentication must not be permitted.

3.14.2 Authentication should take place external to an application, i.e., applications should NOT implement their own authentication mechanism. External authentication services should be relied upon.

3.14.3 Passwords must not be stored in clear text.

3.14.4 Role-based access controls should be used whenever feasible, in order to support changes in staff or assigned duties.

3.14.5 Where technically or administratively feasible, systems should allow for lock-outs after a set number of failed attempts. Lock-outs should be logged unless the log information includes password information.

3.15 Email Identification

3.15.1 Where technically or administratively feasible, agencies may require Agency Identifiers in an email address account. An Agency Identifier is a 3-5 letter acronym representing the Agency's name.

3.15.2 Agencies may request an Identifier added to email addresses, in a format approved by WVOT, when:

3.15.2.1 Employees transfer OUT of the requesting Agency to the employment of another agency within West Virginia state government;

3.15.2.2 Employees transfer IN to the requesting Agency from the employment of another agency within West Virginia state government;

3.15.2.3 A new employee email account is created; or

3.15.2.4 In order to standardize all agency email accounts.

4.0 RELEVANT MATERIALS/DOCUMENTS

This policy is consistent with the following federal and state authorities:

- 45 Code of Federal Regulations (CFR) §§ 164.308-316
- Freedom of Information Act
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Privacy Rule
- NIST SP 800-14 and NIST SP 800-53
- State Health Privacy Laws
- WV Code § 5A-6-4a
- WV Executive Order No. 7-03
- WVOT Policies Issued by the Chief Technology Officer (CTO), www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

5.0 ENFORCEMENT & AUTHORITY

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the **West Virginia Division of Personnel**. Please review the **WVOT Policy and Procedure Policy #1000** to review additional provisions concerning enforcement and policy authority.

6.0 POLICY-SPECIFIC DEFINITIONS

6.1 Access– The ability to locate, gain entry to, and use a directory, file, or device on a computer system or over a network.

6.2 Access Controls – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

6.3 Authentication – The process of verifying the identity of a user.

6.4 Procedure – A defined series or sequence of steps followed in a definite regular order ensuring the consistent and repetitive approach to actions.

6.5 User – A person authorized to access an information resource.

7.0 Change Log History

- January 30, 2015 –
  - Changed Section 3.1 to read, "The WVOT is responsible for adding, modifying, and deleting network users' account access for Executive Branch agencies. Name changes, accounting changes, and permission changes are all documented."; Deleted repetitive Section 3.5, "The use of shared accounts is prohibited, unless authorized by the WVOT. Each account must have a designated owner who is responsible for the management of access to that account and for maintaining a list of individuals who have access to the shared account."
- July 1, 2015 –
  - Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions;
- 9/1/2016
  - Added sections 3.12- 3.15
- 10/20/2017 – Policy reviewed. No edits made.

State of West Virginia Office of Technology Policy:
IT Policy and Procedure Development

Issued by the CTO

1.0 PURPOSE

This policy establishes the form and content criteria for the West Virginia Office of Technology (WVOT) regarding information technology (IT) policy and procedure development, maintenance, and distribution to agencies within the State of West Virginia Executive Branch.

2.0 SCOPE

This policy applies to all employees engaged in developing technology policies or procedures, unless classified as "exempt" in West Virginia Code Section 5A-6-8, "Exemptions." The State's users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Instant Messaging services.

3.0 POLICY

3.1 Every employee is responsible for abiding by all State IT policies and relevant procedures.

3.2 State employees may view all policies by accessing the WVOT Internet policy page at: go.wv.gov/wvotpolicies

3.3 Agency Responsibilities

3.3.1 Agencies may establish more stringent IT policies; however, duplication of content should be avoided.

3.3.2 Each agency developing a security policy supplement **must** submit it to the WVOT for review.

3.3.3 Agency management is responsible for communicating IT policies and procedures to all current State employees.

3.3.4 Each agency will designate an individual who will be responsible for reviewing all policies and procedures, if applicable, with all newly transferred and hired employees.

3.4 WVOT Responsibilities

3.4.1 The WVOT Policy Unit within the Cyber Security Office (CSO) is responsible for developing and maintaining effective IT and Information Security policy and procedure. This Unit works closely with interested and affected individuals, technical editors, and subject matter experts, as needed.

3.4.2 The WVOT is responsible for establishing and coordinating IT policies and procedures. Final authority for WVOT policies falls to the CTO.

3.4.3 Both State IT policies and procedures are defined by a set of criteria in order to provide consistency and to comply with the multiple local, state, and federal regulations that need followed for compliance.

3.5 Review and Modification

3.5.1 The WVOT will designate an individual(s) to review and amend (as needed) IT policies and procedures annually.

3.5.2 Substantive changes to policy or procedure may only be made with CTO approval.

3.5.3 When revisions to a policy or procedure are necessary, the CTO will determine whether the changes will require a global notification.

3.5.4 Approved policies and procedures remain in effect and are only replaced at the release of a new or modified document.

3.5.5 Any modified or temporary policy or procedure that materially affects the usage rights or responsibilities of employees will be communicated to agencies by a global e-mail message alert or ISA contacts.

3.6 Issues that may trigger policy creation, review, or modification include:

3.6.1 Recognition of a need (for example, legislative requirement, audit outcomes);

3.6.2 Changes in strategic direction and plans;

3.6.3 The Policy and Procedure Development and Review Schedule or an accumulation of issues logged with the Manager;

3.6.4 Identification of content gaps or overlaps across or between policies; or,

3.6.5 The review date of the policy.

3.7 Emergency Temporary Policies

3.7.1 Under certain conditions, the CTO may need to set emergency temporary policies, which will take effect immediately.

3.7.2 The emergency temporary policy will remain in effect for 180 calendar days from the date signed by the CTO. The date may be extended as necessary.

3.8 Maintaining Policies and Procedures

3.8.1 Any State employee may either request that a new IT policy or procedure be written, or propose that revisions to an existing document be made.

3.8.2 Policies and procedures related to information and data system security are reviewed annually, updated as needed, and approved by the relevant department, CISO, and then by the CTO.

3.8.3 The WVOT is responsible for posting and maintaining all IT policies on the State's policy web page: (www.technology.wv.gov). Procedures will be posted to the Intranet only.

3.8.4 To ensure consistency, the WVOT has created a standard format for both policies and procedures to facilitate the adoption of clear, concise documents at all levels of State agencies.

3.9 Authority

3.9.1 Under the provisions of West Virginia Code §5A-6-4a *et seq.*, the Chief Technology Officer (CTO) is charged with securing State government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats.

3.9.2 The CTO is granted both the authority and the responsibility to develop information technology policy, promulgate that policy, audit for policy compliance, and require corrective action where compliance is found to be unsatisfactory or absent.

3.9.3 This policy is one in a series of IT-related policies intended to define and enable the incorporation of appropriate practices into all activities using State-provided technology in the State of West Virginia.

3.9.4 To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy.

3.9.5 In instances where existing state and federal laws and regulations are more restrictive than information security policies issued by the WVOT the more restrictive provisions will prevail.

3.10 Enforcement Powers

3.10.1 Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal.

3.10.2 Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the West Virginia Division of Personnel.

3.10.3 Violations of this policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

3.10.4 The State may also be required by law to report certain illegal activities to the proper law enforcement agencies.

4.0 RELEVANT MATERIALS/DOCUMENTS

This policy is consistent with the following federal and state authorities:

- 45 Code of Federal Regulations (CFR) §§ 164.308-316
- Freedom of Information Act
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Privacy Rule
- NIST SP 800-14 and NIST SP 800-53
- State Health Privacy Laws
- WV Code § 5A-6-4a
- WV Executive Order No. 7-03
- WVOT Policies Issued by the Chief Technology Officer (CTO), www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

5.0 ENFORCEMENT & AUTHORITY

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the **West Virginia Division of Personnel**. Please review Sections 3.9 and 3.10 of this policy to review additional provisions concerning enforcement and policy authority.

6.0 FULL POLICY DEFINITIONS

6.1 Access Controls – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

6.2 Access– The ability to locate, gain entry to, and use a directory, file, or device on a computer system or over a network.

6.3 Anti-Virus Coordinator – The person designated by the CTO to monitor and coordinate anti-virus activities within Executive Branch agencies.

6.4 Anti-Virus Software – Software that defends a PC against viruses and other malicious Internet code by scanning incoming attachments in e-mail and from other programs.

6.5 Anti-Virus Team Lead – The functional supervisor of the Anti-Virus Team.

6.6 Authentication – The process of verifying the identity of a user.

6.7 Back-up Files – Electronic files created to restore system files that have become inaccessible on a system.

6.8 Business Records - A document that is used to store information from business operations. Types of operations having business records include meetings and contracts, as well as transactions such as purchases, bills of lading and invoices. Business records can be stored as reference material and reviewed later

6.9 Certification - Certification is an evaluation process assessing non-technical and technical security management, operations, and technical controls, policy, and requirements. Together with a risk analysis and a vulnerability assessment, certification produces documents that support management decisions.

6.10 Certification and Accreditation (CaA) – Validation process that insures that the West Virginia Office of Technology validates the security readiness for devices, systems, software, and other technology prior to deployment of technology into a production status. This validation includes appropriate reviews and/or testing of configurations, hardening, functionality and compliance with specifications, regulations, standards and objectives the generated the deployment activities.

6.11 Change Requesters -- This may be anyone who requests a change to an information system. For example, the Change Requester for an application program modification may be an application analyst. The Change Requester for a change to the computer room will be the Director of Computer Operations or the Director's designee.

6.12 Chief Information Security Officer (CISO) – Person designated by the CTO to oversee information security practices and initiatives for the Executive Branch of WV State government, excluding the constitutional officers.

6.13 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

6.14 Compromise - a vulnerability that has been found and exploited by an unauthorized user.

6.15 Computer Virus – A piece of potentially malicious software that is designed to cause some unexpected or undesirable event, and is generally introduced to a system without the knowledge or consent of the user.

6.16 Confidential Data – Information that is legally protected (ex: Protected Health Information) or otherwise deemed by a qualified expert to be unsuitable for open access.

6.17 Configuration Management Team – A team within WVOT responsible for making changes to the computer and network architecture.

6.18 Contractor – Anyone who has a contract with the State or one of its entities.

6.19 Criticality - Being of the highest importance. The level at which it data must be protected from non-recovery.

6.20 Custodian of Information – The person or unit assigned to supply services associated with the data.

6.21 Data owner – The entity having primary responsibility for the creation and maintenance of the data content.

6.22 Encryption -- An effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

6.23 E-mail – The transmission of messages over communications networks.

6.24 E-mail System – A service that sends messages on devices via local or global networks. E-mail systems provide for storage, and later retrieval of messages and attachments, as well as real-time communication.

6.25 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of information technology and security policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.

6.26 Enterprise Change Management Committee - Consists of directors and managers from multiple areas of WVOT, who make appropriate determinations

6.27 Freedom of Information Act (FOIA) - A federal law that mandates that all the records created and kept by federal agencies in the Executive Branch of government must be open for public inspection and copying. The only exceptions are those records that fall into one of nine exempted categories listed in the statute.

6.28 Health Insurance Portability and Accountability Act (HIPAA) – A US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers. Developed by the Department of Health and Human Services, these standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed.

6.29 Individual Contracts – Contracts with individuals for the purpose of providing a specific product or service to the State.

6.30 Information Assets – Any of the data, hardware, software, network, documentation, and personnel used to manage and process information.

6.31 Information Resources – Any information in electronic, audio-visual or physical form, or any hardware or software that makes possible the storage and use of information.

6.32 Information Security – Those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.

6.33 Information Security Administrator (ISA) – The person designated by the agency head to assure the agency's compliance with State information security policies and procedures. The ISA is the agency's internal and external point of contact for all information security matters.

6.34 Information Security Incident – An event characterized by unexpected and unwanted system behavior, breach, or unintended alteration of data.

6.35 Information Security Liaison (ISL) - Employees assigned by the ISA to assist in the protection of information resources.

6.36 Information Technology (IT) – The technology involved with the transmission and storage of information, especially the development, installation, implementation, and management of computer systems and applications.

6.37 Informational E-mail Messages – Messages that are generally of temporary value, consisting of content created primarily for the informal communication of information.

6.38 Instant Messaging (IM) – The technology that allows a user to send electronic messages to one or more persons with minimal delay between the sending and receipt of a message. Like conversation, IM is a simultaneous give-and-take, but it occurs in written form. In contrast to e-mail, which remains unread in a recipient's in-box until opened; instant messaging notifies users when other users are online and able to accept messages.

6.39 Internet - A publicly accessible system of networks that connects computers around the world via the TCP/IP protocol.

6.40 IT Policy – Written statements defining requirements and compliance mandates in the conduct of employees of the State of West Virginia. Only the CTO may issue policy statements relating to IT.

6.41 ITECH Contractors – A list of pre-approved vendors used by the State, who compete for individual staffing needs based upon criteria developed by the agency and the WVOT.

6.42 Just Cause – a legal and legitimate reason.

6.43 Mass Mailings – Information shared with a group of people who all need to know the same material, (ex., committee members, individual units within Bureaus, etc.).

6.44 Medium – Any repository, including paper, used to record, maintain, or install information or data.

6.45 Network Backbone – The physical and electronic network infrastructure, currently under the operational administration of the WVOT.

6.46 Network Violation Report (NVR) – A summary of 24 hours of activity supporting the contention that a serious policy violation has occurred.

6.47 Cyber Security Office (CSO)) - The functional unit charged with the responsibility to undertake and sustain initiatives to promote, enhance, monitor, and govern actions, standards, and activities necessary to safeguard data and information systems within the Executive Branch of WV, as provided in West Virginia Code §5A-6-4a and the Governor's Executive Order No. 6-06.

6.48 Open Network – An area that allows persons using laptop computers equipped with wireless network cards to connect to the WVOT network, via a VPN.

6.49 Owner of Information – The person(s) ultimately responsible for an application and its data viability.

6.50 Password – A string of characters known to a computer system or network and to a user who must enter the password in order to gain access to an information resource.

6.51 Peer-to-Peer Software (P2P) – A type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives.

6.52 Personally Identifiable Information (PII) –Includes all protected and non-protected information that identifies, or can be used to identify, locate, or contact an individual.

6.53 Privacy Officer - The official responsible for facilitating the Executive Branch's integration of privacy principles, legal requirements, and privacy standards into department policies, procedures, and practices.

6.54 Procedure – A set of instructions or process steps prescribed in sufficient detail in order to understand how to meet a policy requirement. Procedures should document roles, methods, options, and examples necessary for a reader to understand how to comply with a policy.

6.55 Retention Interval – Specifies how long the e-mail (sent or received) needs to be kept to satisfy administrative, legal, fiscal, and historical requirements.

6.56 Risk – The evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.

6.57 Risk Analysis – The evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.

6.58 Scan – To examine computer coding/programs sequentially, part by part. For viruses, scans are made for virus signatures or potentially unsafe practices (e.g., changes to an executable file, direct writes to specific disk sectors, et. al.).

6.59 Secured ("Closed") – An area that allows State personnel using laptop computers equipped with wireless network cards to connect to the WVOT network directly. A network reserved for State of West Virginia employees and agencies. These wireless networks require password

6.60 Security Contact – These individuals include the ISA or the ISL.

6.61 Sensitivity - The level at which data must be protected from disclosure.

6.62 Social Media – Social media includes web- and mobile-based technologies which are used to turn communication into interactive dialogue among organizations, communities, and individuals. Examples are Facebook, MySpace, Twitter, YouTube, etc.

6.63 Social Networking – In the online world social networking is the term used to describe the way that users build online networks of contacts and interact with these personal or business friends in a secure environment. Some of the most popular social networking sites include Facebook and Twitter.

6.64 SSID – A Service Set Identifier is a name that identifies a wireless network. All devices on a specific wireless network must know its SSID.

6.65 State Records – Documentary materials or information, regardless of physical media or characteristics, made or received by an office in connection with the transaction of official business, and preserved by that office as evidence of the State's functions, policies, decisions, procedures, operations, or other activities of that office, or because of the value of the data in the record. These messages can set policy, establish guidelines or procedures, capture a dialogue, certify a transaction, or become a receipt.

6.66 State-Use Contracts – Contracts with specific outside companies to provide custodial services to State agencies.

6.67 System – A combination of hardware, software, and procedures necessary to support particular data. A server may have multiple systems and a system may require multiple servers.

6.68 System Owner - The entity who has overall responsibility for a computer application. This person might be required to approve design changes, updates, new reports, system access, or any other action pertaining to the disposition of the application, or data associated with that application. This person would be a subject matter expert (SME) on the system's purpose, hardware requirements, communications requirements, funding requirements, user criteria, etc.

6.69 Temporary Services Contracts – Contracts with temporary service agencies, which offer clerical or secretarial assistance.

6.70 Terms of Service (TOS) – Rules by which one must agree to abide in order to use a service. It is generally assumed such terms are legally binding.

6.71 Threat – Includes any person, condition, or circumstance that endangers the security of information or information systems in the context of information security.

6.72 USB Drive – A plug-and-play portable storage device that uses flash memory and is lightweight enough to attach to a key chain. A USB drive can be used in place of a floppy disk, Zip drive disk, or CD.

6.73 User – A person authorized to access an information resource.

6.74 User ID – A unique "name" by which each user is identified to a computer system.

6.75 Web – World Wide Web means the complete set of documents residing on all Internet servers that use the HTTP protocol, accessible to users via a simple point-and-click system. Sometimes the WEB and "Internet" are used as if they mean the same thing, however, the Internet is actually the network infrastructure that supports the WEB.

6.76 West Virginia Division of Personnel – A division of the Department of Administration established by West Virginia Code § 29-6-1 *et seq.*, which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.

6.77 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, *et. seq.*, which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

6.78 Wireless Access Point - Any piece of equipment that allows wireless communication using transmitters and receivers to enable communications.

6.79 Workstation – A personal computer; also called a PC.

6.80 WVOT Policy Unit - The Unit responsible for developing and maintaining IT and/or Information Security policy and procedure.

7.0 CHANGE LOG

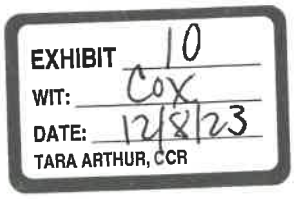
- July 1, 2015 –
  - Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; compiled all policy definitions; made all references to timelines one year; Added Authority and Enforcement Sections 3.9 and 3.10; Added list of reasons for policy create, modification, or review in Section 3.6; Added information about compliance regulations in Section 3.4.3.
- 9/1/2016
  - Policy Reviewed, no edits made.
- 10/20/2017
  - Policy Reviewed, no edits made.

Disability Rights WV

December 20, 2022

VIA EMAIL: DHHRSecretary@wv.gov

Dr. Jeffrey Coben, M.D.
Interim Cabinet Secretary
West Virginia Department of
Health and Human Resources
One Davis Square, Suite 100 East
Charleston, West Virginia 25301



RE: NOTICE TO PRESERVE DOCUMENTS & ELECTONRICALLY-STORED INFORMATION

Dear Dr. Coben:

At Mr. Crouch's request on December 6, 2022, DRWV accepted his invitation to have collaborative discussions with DHHR to attempt to move forward in a positive manner. DRWV remains willing to work cooperatively with DHHR to identify issues and develop solutions to promote and protect the rights and needs of persons with disabilities. Likewise, DRVW welcomes the opportunity to assist you as you deem appropriate. DRWV is aware of the challenges you face and respectful of the daunting issues you are confronting.

While DRWV remains committed to exploring a resolution of issues with DHHR in good faith, DRWV also recognizes the increasing need and compelling urgency to protect vulnerable persons with a disability. As such, in anticipation of DRWV providing notice in accordance with W.Va. Code §55-17-3 of likely suit against DHHR, as defined herein, and others, DRWV respectfully demands that you and DHHR preserve all documents, tangible things and electronically stored information potentially relevant to the issues identified below ("Likely Litigation Issues" and "Search Phrases"). This demand is in addition to my December 12, 2022, email to April Robertson to preserve certain cell phones and all data on such cell phones.

As used in this document, "you" and "your" and "DHHR" means the West Virginia Department of Health and Human Resources, its agents, attorneys, accountants, employees, contract workers, consultants, partners or other persons occupying similar positions or performing similar functions, including, but not limited to, current and former members of DHHR's Leadership team, the DHHR Secretary, Bureau Commissioners, Office Directors, General Counsel, and Director of the Office of Communications ("Senior Officials"), and all persons who are directly supervised by or report to any of the Senior Officials.

Likely Litigation Issues:

1. Civil conspiracy by and among certain persons employed by or affiliated with DHHR, including Bill J. Crouch and Shevona Lusk, to withhold, conceal, or deny access to documents and information or withhold, conceal, or deny access to documents and information by unlawful means and/or to impair, impede, or frustrate DRWV's independent and federal statutory authority to monitor state health care facilities and receive documents and information related to patients or health care service delivery at state health care facilities in violation or likely violation of the P&A Acts. *See generally* 42 U.S.C §§ 15043(a)(2)(I) and (J); 42 U.S.C. § 10805(a)(4); 42 CFR § 51.41; 62 FR 53548-01, 1997 WL 630749(F.R.); and W.Va. C.S.R. §64-59-20; *see also Dunn v. Rockwell*, 689 S.E.2d 255, syl. no. 8 (W.Va. 2009) ("A civil conspiracy is a combination of two or more persons by concerted action to accomplish an unlawful purpose or to accomplish some purpose, not in itself unlawful, by unlawful means. The cause of action is not created by the conspiracy but by the wrongful acts done by the defendants to the injury of the plaintiff.").

2. DHHR's failure to monitor and appropriately enforce existing policies, procedures, contracts, grant agreements, and provider agreements involving (a) Comprehensive Behavioral Health Centers; (b) Community Engagement Specialist(s); (c) The Intellectual/Developmental Disabilities Waiver (IDDW) program; (d) Kepro and/or Kepro's West Virginia Administrative Services Organization; and (e) providers of services to individuals with developmental disabilities in the community and in group homes that has resulted in, contributed to, and/or permitted the improper placement of persons with a disability, the unnecessary institutionalization of persons with a disability, an absence of required community-based services to prevent otherwise avoidable institutionalization, participant and patient dumping by community-based providers that unnecessarily clogs hospital emergency departments and mental health facilities, deficient service delivery, overcrowding of state mental health facilities, and the lack of less restrictive placements for persons with developmental disabilities.

3. DHHR's failure to monitor and enforce the provisions of the IDDW Manual, especially WV BMS Policy (513.27 Transfer), that has resulted in discriminatory practices and outcomes, dumping of participants who are developmentally disabled, unnecessary and avoidable institutionalization of persons with a developmental disability, and squandering public resources.

4. DHHR's failure to require sufficient levels of performance reviews and audits of providers of services for the Intellectual/Developmental Disabilities Waiver (IDDW) program that has resulted in or contributed to a failure to provide required services to persons with a developmental disability, wasted public resources, and the absence of standards to maintain sufficient less restrictive placements and appropriate service delivery.

5. DHHR's lack of standards or protocols for imposing appropriate disallowances and penalties for noncompliance by IDDW providers.

6. DHHR's lack of enforcement of program integrity that permits deficient service delivery to IDDW participants and diminished accountability of IDDW providers.

7. DHHR's failure to provide sufficient Assertive Community Treatment services that are a proven, evidence-based intervention that prevents re-admissions and targets individuals at risk of hospitalization.

8. DHHR's failure to provide services, failure to oversee the provision of services, and failure to dedicate sufficient resources and staff to provide services required by 42 U.S.C. § 300x-2(c)(1)(B) ("Outpatient services, including specialized outpatient services for children, the elderly, individuals with a serious mental illness, and residents of the service areas of the centers who have been discharged from inpatient treatment at a mental health facility.").

9. DHHR's failure to provide services, failure to oversee the provision of services, and failure to dedicate sufficient resources and staff to provide services required by 42 U.S.C. § 300x-2(c)(1)(C) ("24-hour-a-day emergency care services.").

10. DHHR's failure to provide services, failure to oversee the provision of services, and failure to dedicate sufficient resources and staff to provide services required by 42 U.S.C. § 300x-2(c)(1)(D) ("Day treatment or other partial hospitalization services, or psychosocial rehabilitation services.").

11. DHHR's failure to provide services, failure to oversee the provision of services, and failure to dedicate sufficient resources and staff to provide services required by 42 U.S.C. § 300x-2(c)(3) ("Services are available and accessible promptly, as appropriate and in a manner which preserves human dignity and assures continuity and high-quality care.").

12. The failure of William R. Sharpe, Jr., Hospital to provide required court-ordered services to persons with a developmental disability who have been committed to Sharpe Hospital and the failure of Sharpe Hospital to take actions that promote the active discharge of such persons.

13. The failure of the Office of Health Facility Licensure and Certification to comply with W.Va. C.S.R. §64-59-1 *et seq.*, and W.Va. C.S.R. §64-12-1 *et seq.*, and allow the state mental health facilities to operate without a license.

14. The failure to place current geriatric patients in a diversion psychiatric hospital who meet discharge criteria in a long-term care facility.

Based on this request, you should anticipate that information subject to disclosure or responsive to discovery in this matter is stored on current and former computer systems and other media and devices (including iPads, android tablets, voice-messaging systems, online repositories and cell phones).

Electronically stored information (hereinafter "ESI") should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically or optically stored as:

- Digital communications (e.g., text messages, e-mail, voice mail, instant messaging);
- Word processed documents (e.g., Word, WordPerfect, or Google documents and drafts);
- Spreadsheets and tables (e.g., Excel or Google worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files);
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- Sound Recordings (e.g., .WAV and .MP3 files);
- Video and Animation (e.g., .AVI and .MOV files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Calendar and Diary Application Data (e.g., Outlook PST, Yahoo, blog tools);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs;
- Project Management Application Data;
- Computer Aided Design/Drawing Files;
- Back Up and Archival Files (e.g., Zip, .GHQ); and
- Cloud/Internet data stored on remote servers, computers or other storage devices not in your immediate control that synchronize with, or are accessible from, one or more devices used by you or members of DHHR including any recoverable deleted data available at the time of receipt of this notice. For example, by way of illustration and not limitation, these may include Google Drive, Microsoft OneDrive, DropBox, etc.

ESI resides not only in areas of electronic, magnetic and optical storage media reasonably accessible to you, but also in areas you may deem not reasonably accessible. You are obliged to preserve potentially relevant evidence from both these sources of ESI, even if you do not anticipate producing such ESI.

The demand that you preserve both accessible and inaccessible ESI is reasonable and necessary. For good cause shown, a Court may order production of the ESI, even if it finds that it is not reasonably accessible. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive DRWV of its right to secure the evidence or the Court of its right to adjudicate the issue.

In addition to the foregoing Likely Litigation Issues, this request also encompasses all ESI that mentions or makes reference to any of the following names, terms, or phrases for the period beginning August 15, 2022 (collectively "Search Phrases"): "DRWV"; "Disability

Rights"; "Disability Rights of West Virginia"; "Disability Rights of WV"; "Parmer"; "Given"; "Thorn"; "Folio"; "White"; "P&A"; "protection and advocacy"; "watchdog"; "advocates"; "IDD" and "audit"; "IDD" and "Sharpe"; "IDD" and "Bateman"; "IDD" and "waiver"; "IDDW"; "WVPB"; "West Virginia Public Broadcasting"; "Butch Antolini"; "Larry Pack"; "PAIMI"; "PADD"; "513.27 Transfer"; "census" and state health care facility; "Sharpe patient census"; "CMS" and "Sharpe"; "CMS" and "Bateman"; "Medley"; "Hartley"; "Ryan"; "Lusk"; "retraction"; "crisis stabilization"; "comprehensives"; "CMHC"; "ICF"; "Kinneberg"; "Sharpe" and "staffing"; "Sharpe" and "COVID"; "Sharpe license"; "W.Va. Code 16-5B-1"; and "informant."

This request also encompasses all ESI exchanged by or among April Robertson, Sheila Lee, Tina Wiseman, Jessica Whitmore, and/or Sarah Harrah that references the Likely Litigation Issues and/or the Search Phrases.

Preservation Requires Immediate Intervention

You must act immediately to preserve potentially relevant ESI including, without limitation, information concerning:

1. The events and causes of action described in Likely Litigation Issues or that mention any of the Search Phrases;

2. ESI you may use to support allegations in Likely Litigation Issues or that mention any of the Search Phrases; and

3. ESI that you may use to support defenses to Likely Litigation Issues or that mention any of the Search Phrases.

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. Be advised that sources of ESI are altered and erased by continued use of your computers and other devices. Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI.

Nothing in this demand for preservation of ESI should be understood to diminish your concurrent obligation to preserve document, tangible things and other potentially relevant evidence.

Suspension of Routine Destruction

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation,

operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure or encryption utilities or devices;
- Overwriting, erasing, destroying or discarding back up media;
- Re-assigning, re-imaging or disposing of systems, servers, devices or media;
- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server or IM logging; and,
- Executing drive or file defragmentation or compression programs.

Preservation in Native Form

You should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, you should preserve ESI in such native forms, and you should not select methods to preserve ESI that remove or degrade the ability to search your ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation.

You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

Metadata

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access.

Application metadata is information automatically included or embedded in electronic files but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields.

Servers

With respect to servers like those used to manage electronic mail (e.g., Microsoft Exchange, Lotus Domino) or network storage (often called a user's "network share"), the complete contents of each user's network share and e-mail account should be preserved.

Home Systems, Laptops, Online Accounts and Other ESI Venues

While DRWV expects that you will act swiftly to preserve data on office workstations and servers, you should also determine if any home or portable systems may contain potentially relevant data. Upon information and belief, DHHR Senior Officials (including Mr. Crouch) have or had a home or portable system that likely contains potentially relevant data. To the extent that DHHR have sent or received potentially relevant e-mails or created or reviewed potentially relevant documents, you must preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CD-R disks and the user's android, smart phone, voice mailbox or other forms of ESI storage.). Similarly, if DHHR used online or browser-based email accounts or services (such as AOL, Gmail, Yahoo Mail or the like) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted and Archived Message folders) should be preserved.

Ancillary Preservation

You must preserve documents and other tangible items that may be required to access, interpret or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID and password rosters or the like.

You must preserve any passwords, keys or other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals and license keys for applications required to access the ESI.

You must preserve any cabling, drivers and hardware, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar code readers, Zip drives and other legacy or proprietary devices.

Paper Preservation of ESI is Inadequate

As hard copies do not preserve electronic searchability or metadata, they are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

Agents, Attorneys and Third Parties

Your preservation obligation extends beyond ESI in your care, possession or custody and includes ESI in the custody of others that is subject to your direction or control. Accordingly, you must notify any current or former agent, attorney, employee, custodian or contractor in

possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

System Sequestration or Forensically Sound Imaging

In the event you deem it impractical to sequester systems, media and devices, we believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As we anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, we demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By "forensically sound," we mean duplication, for purposes of preservation, of all data stored on the evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the original. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including in the so-called "unallocated clusters," holding deleted files.

Confirmation of Compliance

You should not defer preservation steps pending such discussions if ESI may be lost or corrupted as a consequence of delay. Failure to preserve potentially relevant evidence could result in the corruption, loss or delay in production of evidence to which we are entitled. Please confirm by letter, that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

Please contact me if you have any questions about this matter. In the interim, please feel free to contact us if you wish to explore collaborative initiatives to promote and protect our vulnerable population.

Very truly yours,

Michael J. Folio
Legal Director

Cc: Cammie Chapman (Cammie.L.Chapman@wv.gov)
Christina Mullins (Christina.R.Mullins@wv.gov)
Russell Crane (Russell.Crane@wv.gov)
Jessica Hudson (DHHRCommunications@wv.gov)
Justin Davis (Justin.J.Davis@wv.gov)

Rae Bates (Rae.J.Bates@wv.gov)
Nicholas Stuchell (Nicholas.R.Stuchell@wv.gov)
Cynthia Beane (Cynthia.E.Beane@wv.gov)
Shevona Lusk (Shevona.R.Lusk@wv.gov)
Sheila Lee (Sheila.R.Lee@wv.gov)
Allison Adler (Allison.C.Adler@wv.gov)
April Robertson (April.L.Robertson@wv.gov)

From: Michael Folio
To: April Robertson; Bates, Rae J; Shevona.r.lusk@wv.gov; Ryan, Patrick W
Cc: Susan Given
Subject: Electronic Data Preservation
Date: Monday, December 12, 2022 3:26:09 PM
Attachments: image001.png

April – Given Mr. Crouch's resignation announcement, and while DRWV remains committed to exploring a resolution of issues with DHHR as Mr. Crouch requested and will work in good faith to resolve such issues, I must ask that you preserve the cell phones and all data on the cell phones of Mr. Crouch and Rae Bates. Ms. Bates has two cell phones that she routinely used for DHHR business – (304) 545-6669 and (304) 590-4425.

I must further ask that you preserve the cell phones and all data on the cell phones of Shevona Lusk (304) 549-1280; Patrick Ryan (304) 203-7654; and your cell phone (304) 590-1397.

I must further ask that you preserve the cell phone and all data on the cell phone of Jolynn Marra that was provided by DHHR and/or the state of West Virginia.

DRWV will be providing a detailed notice to preserve electronically stored information in connection with a notice to file suit in the coming days.

Thank you.

Mike

Michael Folio, Legal Director

Disability Rights WV

Disability Rights of West Virginia
Removing Barriers to Opportunity and Equality

800.950.5250 *(toll free)*

304.346.0847 *(voice/tty)* • 304.346.0867 *(fax)*
5088 Washington St W, Ste 300• Charleston, WV 25313
drofwv.org